MEBERUFE info

UNTERRICHTSMODUL SICHERHEIT IM INTERNET

SICHERHEIT IM INTERNET

ARBEITSBLATT UND LEHRERINFORMATION

Fachinhalte:

- Persönlichkeits- und Urheberrecht
- Datenschutz und -sicherheit
- Schadprogramme wie Viren, Trojaner, Malware
- Zugriffs- und Zugangskontrolle
- Passwörter, Verschlüsselung, PIN
- Persönlichkeits- und Bewegungsprofile im Internet
- Sicherheits-Apps, Backup, Updates

Herausgeber: Arbeitgeberverband Gesamtmetall

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

HAUSAUFGABE

Lösungsvorschlag:

Mein Smartphone ...	Ja/Name/Funktion/Wann?	Nein
... ist immer unter Aufsicht und bei mir.	Ja	
... hat eine Bildschirmsperre.	Ja, PIN / Fingerabdruck, Muster-PIN	
... hat die SIM-Karte per PIN-Abfrage geschützt.	Ja, die PIN-Abfrage ist aktiviert.	
... verwendet sichere Passwörter.	Ja, niemals persönliche Daten wie Geburtstag oder 0000, 1111, 1234.	
... hat gerade ein Sicherheits-Software-Update aktualisiert.	Ja, in dieser Woche.	
... hat eine Antivirus-App installiert.	Ja, kostenlose App, z. B. McAfee oder Avast.	
... hat nur Apps aus dem offiziellen Play-/App- Store installiert.	Ja, ich habe in „Einstellungen“ die Installation von Apps unbekannter Herkunft blockiert.	
... hat alle Apps auf dem aktuellen Stand.	Ja, ich mache regelmäßig anstehende Updates.	
... hat Bluetooth, WLAN und GPS-Ortung nur, wenn ich es aktiviere.	Ja, ich aktiviere diese Funktionen bewusst unter „Einstellungen“, wenn ich sie nutzen möchte.	

EINSTIEG UND MOTIVATION

Lösungsvorschlag:

Impuls-Szenario:
Der Besuch einer unseriösen Website oder ein kurzer, unbeaufsichtigter Moment am Handy reicht aus, damit eine Spionage-App, wie z. B. FlexiSpy, illegal installiert werden kann. Nach der Installation verbirgt die App ihre Dateien, sodass die Spionage-App nach außen kaum erkennbar ist. Nur an einem erhöhten Datenvolumen, verkürzter Akku-Laufzeit oder verlangsamten Prozessen könnte man erkennen, dass eine solche App auf dem Smartphone installiert wurde. Zudem sperrt die App ihre Dateien, sodass eine Deinstallation verhindert wird. Die Spionage-App kann alle Aktivitäten wie Chat-Verläufe, Standort-Daten, Anrufprotokolle, Kalendereinträge, Textnachrichten oder die Kamera auslesen und per Internet auf einen Server schicken. Dort können die Inhalte mitgelesen werden.

Mögliche Erfahrungen der Schülerinnen und Schüler:
- Tracking-Apps verfolgen meine Surf-Aktivitäten und Vorlieben im Internet und blenden personalisierte Werbung ein.
- Privater Chat-Verlauf wird als Screenshot weiterverbreitet.
- Private Fotos werden von Dritten ohne Erlaubnis in sozialen Netzwerken veröffentlicht.
- Man erhält Fotos, Videos mit unangenehmen Inhalten (Gewalt, Sex, politischer Extremismus).
- Identitätsdiebstahl und Anmeldung bei Kontaktbörsen unter falschem Namen.
- Durch Klicken eines Links ein Schadprogramm herunterladen.
- Der Aufenthaltsort kann verfolgt werden.
- Hohe Kosten durch Drittanbieter aus Schadprogrammen.
- Falsche Warenbestellungen
- Hohe Mobilfunkrechnung durch Nutzung mobiler Datendienste im Ausland ohne Internet-Flat.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

1. DATENSCHUTZ, DATENSICHERHEIT UND URHEBERRECHT

JURISTISCHE RECHTSPOSITIONEN UND MASSNAHMEN

Lösungsvorschlag:

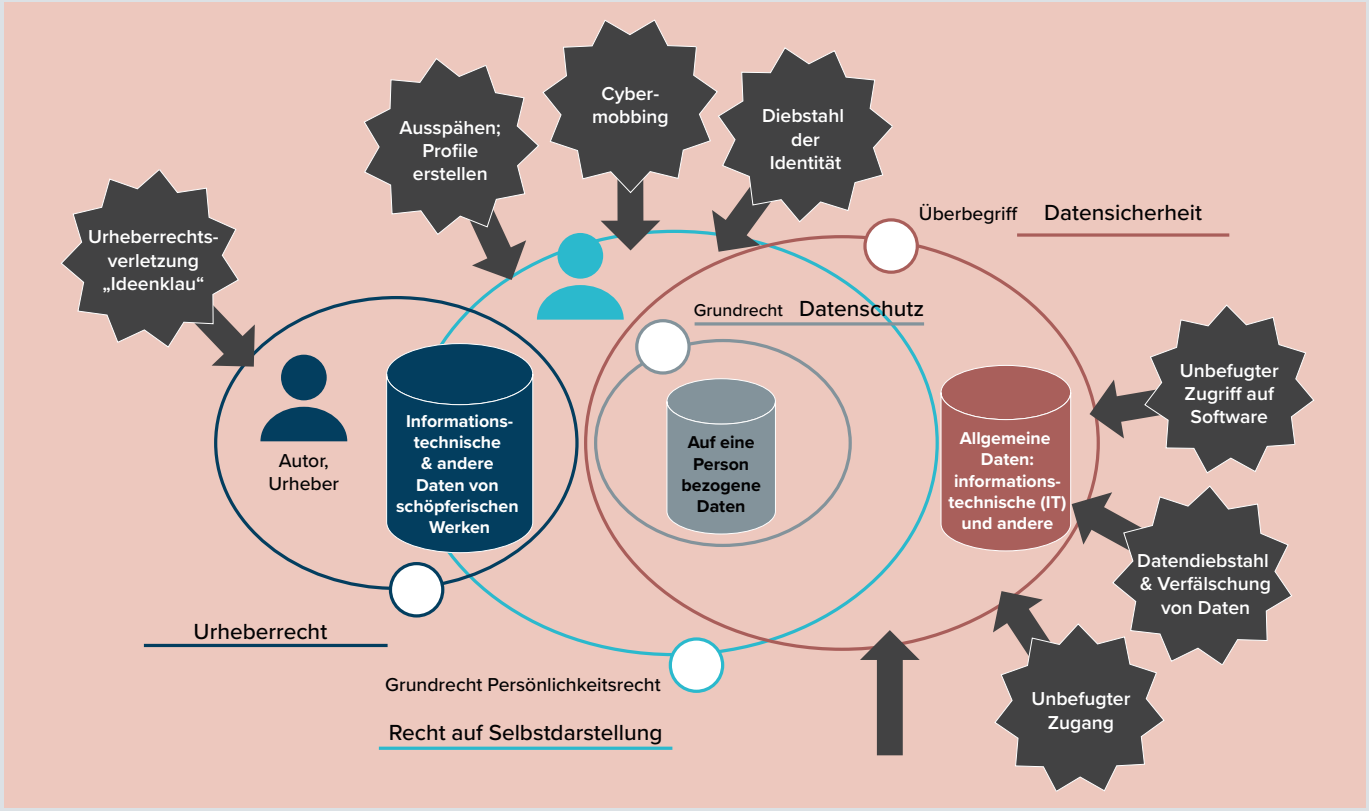
Das Persönlichkeitsrecht ist ein umfassendes Grundrecht und in mehrere Einzelschutzrechte unterteilt. Die verschiedenen Einzelrechte schützen die Persönlichkeit, also das Ansehen, die Ehre und die persönlichen Daten sowohl in der analogen Welt als auch in der digitalen Datenverarbeitung. Es umfasst besonders das **Recht auf Selbstbestimmung** und das **Grundrecht Datenschutz**. Dieses wird auch als das **Recht auf informationelle Selbstbestimmung** bezeichnet.

A	B	C	D
Recht auf Selbstdarstellung	Grundrecht auf Datenschutz	Urheberrecht	Datensicherheit
C	**A**	**B**	**D**
Dieses Recht schützt das geistige Eigentum einer Person an ihren Werken, das sind z. B. Texte, Musik, Bilder oder Fotos. Dazu gehören auch Werke in digitaler Form. Das Recht verhindert, dass andere die Werke des Urhebers ohne dessen Erlaubnis nutzen.	Dieses Recht stellt sicher, dass die Person selbst darüber bestimmt, wie sie sich in der Öffentlichkeit darstellt. Sie entscheidet selbst, wie und ob ihr Name, ihr Bild oder das eigene Wort veröffentlicht wird. Außerdem ist die Ehre geschützt, d. h. niemand darf die Person öffentlich beleidigen oder ihr falsche Aussagen unterschieben.	Dieses Recht stellt sicher, dass eine Person selbst darüber bestimmt, ob und wem sie ihre eigenen, personenbezogenen Daten anvertraut und wie die Daten dann verwendet werden dürfen. Dieses Recht schließt auch die Speicherung und Verarbeitung der Daten in Computersystemen ein.	Dies ist ein Überbegriff für technische und organisatorische Maßnahmen zur Sicherung von Daten. Damit sind alle Daten gemeint, also allgemeine und personenbezogene Daten, analoge Daten (z. B. Akten) aber auch digitale Daten. Die Maßnahmen umfassen Technik und Organisation, um die Daten gegen Bedrohungen zu sichern. Solche Bedrohungen können z. B. Verfälschungen, unerlaubte Einsicht in Daten und die Zerstörung oder der Verlust von Daten sein.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

GELTUNGSBEREICHE DER RECHTE UND MASSNAHMEN

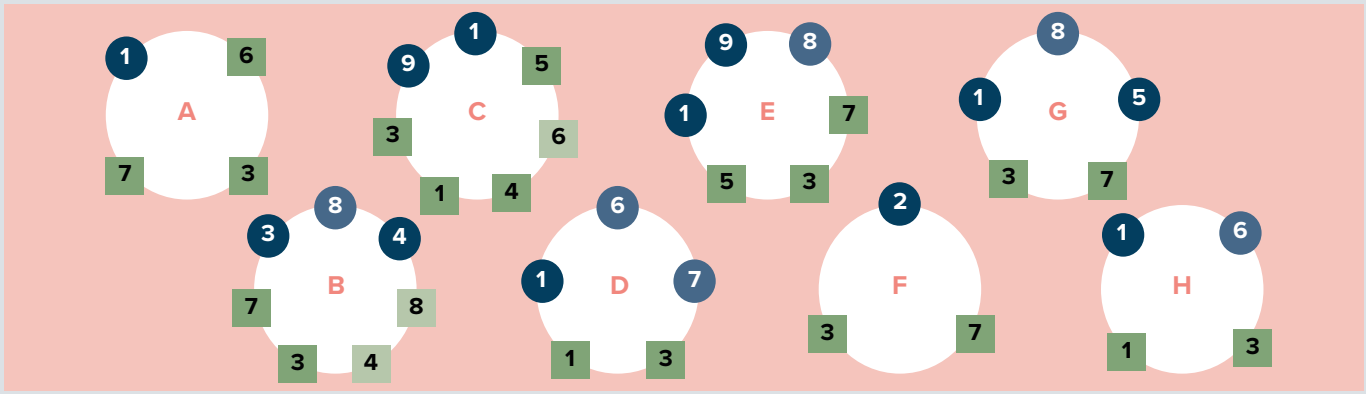
Lösungsvorschlag:



2. SICH IM INTERNET BEWEGEN: RECHTLICHE SICHT UND DATENSICHERHEIT

AKTIVITÄTEN UND DATENKATEGORIEN BEI UP- UND DOWNLOADS

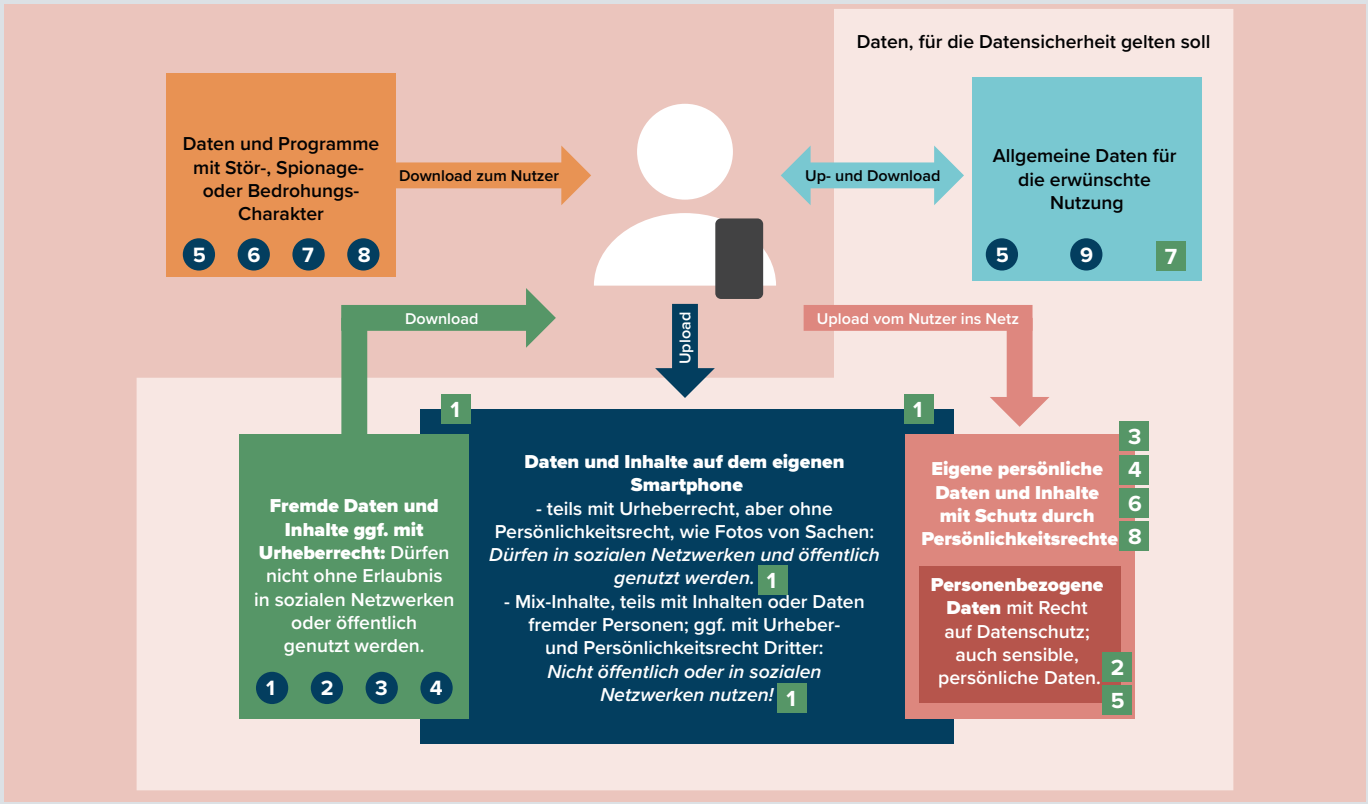
Lösungsvorschlag:



HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

JURISTISCHE SCHUTZRECHTE UND SICHERHEITSBEDINGUNGEN

Lösungsvorschlag:



BONUSAUFGABE: PASSWORT KNACKEN

- Die Entwicklung der Formel: Anzahl der Zeichen N von 0–9 ist N=10 Für jedes Zeichen N_1 an der ersten Stelle kann die zweite Stelle N_2 je 10 Zeichen und die dritte Stelle N_3 auch 10 Zeichen annehmen. Die Stellen multiplizieren sich. Die Anzahl der Kombinationen = N_1*N_2*N_3 = 10*10*10 = 1.000 Möglichkeiten.
- Die Methode zur Verbesserung der Passwort-Sicherheit: Wenn die Zahl der Versuche auf 3 begrenzt wird, ist die Treffer-Wahrscheinlichkeit sehr klein.
- Die Kombinationsmöglichkeiten für größeren Zeichenvorrat: Anzahl der Zeichen N_1 ist a–z = 26, zusätzlich A–Z = 26, zusätzlich 0–9 = 10. An der Stelle N_1 können also insgesamt 62 verschiedene Zeichen auftreten. Dasselbe gilt für N_2 und N_3. Also N_1 = N_2 = N_3 = 62. Die Kombimöglichkeiten jeder Stelle multiplizieren sich, also ergibt sich wie oben: Kombinationsmöglichkeiten: $N\_1*N\_2*N\_3 = (N\_1)^3 = 238.328$. Das sind 237.328 Möglichkeiten mehr als im ersten Beispiel, also rund das 238-fache.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

3. SCHUTZMASSNAHMEN FÜRSMARTPHONE UND NUTZER

BEDROHUNGEN UND RECHTSVERLETZUNGEN

Lösungsvorschlag:

GRUPPE „UPLOAD“

BEDROHUNG	MÖGLICHE RECHTSVERLETZUNG
Unbefugter Zugang - Diebstahl - Unbemerkte Fremdnutzung **ist, wenn ...**	... sich ein Krimineller z. B. in sozialen Netzwerken oder per E-Mail mit falscher Identität ausgibt. Das erlaubt ihm, im falschen Namen einzukaufen, Online-Banking zu machen, den Ruf zu schädigen oder falsche Anrufe zu tätigen.
Datendiebstahl - aus internem oder externem Speicher oder - Verfälschung von Daten **wird möglich, wenn ...**	... unerwünscht eindringende Schadprogramme auf das Software-System zugreifen und es beschädigen. Die Schadprogramme können ferngesteuert werden und geheime Zugangsdaten ausspähen, unbemerkt Sicherheitslücken erzeugen, Daten zerstören und Systemfunktionen beschädigen.
Mit Schadsoftware wie - Virus - Malware - Schadprogrammen **infiziert sich das Smartphone dadurch, dass ...**	... das Opfer durch Messenger-Dienste wie Chats oder Anrufe beleidigt, bedroht oder bloßgestellt wird. Es werden Unwahrheiten und gefälschte Medien verbreitet.
Identitätsdiebstahl bedeutet, dass ...	... das Handy nicht verschlüsselt ist oder externe Speicher wie Datenbanken geknackt, Daten entwendet oder verändert werden. Das sind z. B. Daten wie E-Mail-Adressen oder Daten aus einem Online-Speicher.
Cybermobbing bedeutet, dass ...	... jemand unerlaubt und unbemerkt das Smartphone mit allen Daten nutzt, entwendet oder ausliest. Sensible Daten auf Smartphone und SD-Karte wie Fotos, E-Mails oder Passwörter können unerlaubt kopiert, verarbeitet und verfälscht werden und unbefugten Zugang zu den eigenen Konten ermöglichen.

GRUPPE „DOWNLOAD“

BEDROHUNG	MÖGLICHE RECHTSVERLETZUNG
Ausspähen, d. h. - ausgespäht werden durch Spionage-Apps (Spyware) **liegt vor, wenn ...**	... „Tracker“-Apps auf Webservern sich merken, welche Seiten besucht werden, wie auf der Seite agiert wird und entsprechende personalisierte Werbebanner und Interessenprofile erstellen. Örtliche Bewegungsprofile entstehen durch Sammeln der personenbezogenen Daten aus Online-Aktionen an verschiedenen Orten.
Profile wie - Persönlichkeitsprofil - Bewegungsprofil **werden dadurch erstellt, dass ...**	... Fotos und Mediendaten mit und ohne Abbildung anderer ohne Erlaubnis veröffentlicht und geteilt werden.
Unter der **Urheberrechtsverletzung**, also „Ideenklau“, versteht man, dass ...	... eine Spyware-App das Nutzerverhalten überwacht. Sie hat Zugriff auf Nachrichten, Browserverläufe, Anruflisten und Chats in sozialen Medien.
Datenverlust bedeutet, dass ...	... Daten beabsichtigt oder unbeabsichtigt gelöscht werden, unauffindbar oder zerstört sind.
Eine **Verletzung des Persönlichkeitsrechts anderer** ist, dass ...	... von anderen Personen erstellte Fotos oder Mediendaten ohne Erlaubnis heruntergeladen, gespeichert und getauscht werden. Das gilt auch für Videos und Musik aus illegalen Quellen und für eigene Mix-Produktionen und Collagen aus Vorlagen anderer.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

„INFEKTIONS-“ UND ZUGANGSWEGE / SCHUTZMASSNAHMEN

Lösungsvorschlag:

„INFEKTIONS-“ UND ZUGANGSWEGE
GRUPPE „UPLOAD“

1. Unbefugter Zugang	2. Datendiebstahl	3. Schadprogramme und unbefugter Zugriff auf Software	4. Identitäts-Diebstahl	5. Cybermobbing
• Das Smartphone liegt ohne Aufsicht sichtbar und zugänglich herum. • Es ist keine Bildschirmsperre aktiviert. • Die Daten sind im internen Speicher und auf der SD-Karte unverschlüsselt.	• Daten im internen Handy-speicher und auf der SD-Karte sind nicht ver-schlüsselt. • WLAN- und Bluetooth-Verbindung als Zugang zum Handy.	• Merkwürdige E-Mail oder Social-Media-Nachricht mit Link oder Anhang • Versteckt in Apps von unseriösen Anbietern • Infizierte Website	• Das Abfangen von Zu-gangsdaten zu Online-Accounts, z. B. mit gefälschten E-Mails oder Websites. • Häufig reicht das Wissen von Name, Adresse und Geburtsdatum des Opfers für die falsche Identität aus.	• Fremde legen falsche Identität in sozialen Netz-werken an. • Fremde Personen kennen private Daten von Dritten.
V J B S	G F	O H X U	Q I K L	K T

„INFEKTIONS-“ UND ZUGANGSWEGE
GRUPPE „DOWNLOAD“

6. Ausspähen	7. Profile erstellen	8. Urheberrechtsverletzung	9. Datenverlust	10. Verletzung des Persönlichkeitsrechts
• Die Installation der Spio-nage-App durch Sicher-heitslücken beim Besuch krimineller Websites. • Durch die manuelle Installa-tion durch Fremde.	• Durch umfangreiche Berechtigungen bei Apps oder in den sozialen Netzwerken. • Cookie-Erlaubnis im Browser • Browser-Erweiterung und Tracking-Apps auf der Web-site erfassen Surf-Aktivität und Vorlieben. • Die Standorterfassung durch Bluetooth, WLAN und GPS.	• Von Dritten gemachte Fotos oder Musik werden ohne Erlaubnis weiterver-breitet oder veröffentlicht. • Das kostenloses Herunterladen und Speichern von aktuellen Mediendaten wie Songs oder Filmen von unseriösen, illegalen Websites. • Das Veröffentlichen von eigenen Produktionen mit Versatzstücken aus fremden Medien-Dateien.	• Datenverlust nach „Hard-Reset“. Das Handy wird nach fehlerhaftem Betrieb zurückgesetzt. • Daten werden versehentlich gelöscht. • Das Smartphone geht kaputt.	• Das Veröffentlichen oder Teilen von Fotos und Mediendaten mit und ohne Abbildung anderer ohne deren Erlaubnis in den sozialen Netzwerken oder im Internet.
W A	R M T F	P E C	N	D